На правах рукописи

КОРНЕЕВ Владимир Александрович

НАНОСЕКУНДНАЯ СИНХРОНИЗАЦИЯ ШКАЛ ВРЕМЕНИ ПО МЕТЕОРНЫМ РАДИООТРАЖЕНИЯМ И ЕЕ ПРИЛОЖЕНИЕ К ЗАЩИТЕ ИНФОРМАЦИИ

Специальность 01.04.03 — радиофизика

АВТОРЕФЕРАТ

диссертации на соискание учёной степени

кандидата физико-математических наук

Казань — 2007

Работа выполнена в Государственном образовательном учреждении высшего профессионального образования "Казанский Государственный Университет им. В.И. Ульянова-Ленина".

Научный руководитель:	доктор физико-математических наук, профессор Сидоров Владимир Васильевич
Официальные оппоненты:	доктор физико-математических наук, профессор Белькович Олег Игоревич
	кандидат физико-математических наук, доцент Хузяшев Рустем Газизович
Ведущая организация:	Федеральный научно-производственный центр "Радиоэлектроника" им. В.И. Шимко

Защита диссертации состоится "14" ноября 2007 г. в _____ ч. _____ мин. в ауд. 210 физического факультета на заседании диссертационного совета Д212.081.18 в Казанском государственном университете по адресу: 420008, г. Казань, ул. Кремлевская, 18.

С диссертацией можно ознакомиться в библиотеке Казанского государственного университета.

Автореферат разослан "12" октября 2007 г.

Учёный секретарь диссертационного совета Д212.081.18,
д.ф.-м.н. Карпов А.В.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Объект исследования и актуальность темы. Проблема высокоточной синхронизации шкал времени является одной из актуальных проблем современной науки и техники. На сегодняшний день уже созданы и постоянно совершенствуются системы передачи времени на большие расстояния, обеспечивающие измерения, погрешность которых не превышает наносекунд. Если говорить о наносекундной погрешности, то можно указать на три основных метода передачи времени: 1) Пассивные спутниковые методы (GPS, ГЛОНАСС, точность/стабильность: 10–40 нс / 2–7 нс; GPS Common View: 1–10 нс / 0.1–2 нс) 2) Активные методы, использующие геостационарные спутники (1–5 нс / 0.1–2 нс) 3) Фазовые метеорные системы синхронизации (точность 0.3–0.9 нс). Менее всего разработан в техническом и коммерческом плане метеорный метод передачи времени.

Метеорный метод передачи времени использует встречную передачу запросных и ответных радиосигналов в канале с высокой степенью взаимности условий распространения. Измерения организованы так, что запросный сигнал привязан к шкале времени, а ответный сигнал несет информацию о сдвиге шкал. Имеющиеся на сегодняшний день теоретические оценки и экспериментальные результаты показывают, что метеорный радиоканал для целей синхронизации является весьма перспективным. Это связано с тем, что потенциальная точность одиночных измерений расхождения времени в метеорном радиоканале составляет доли наносекунды и эти измерения не требуют затрат времени на накопление результатов как например в случае GPS/ГЛОНАСС. Перспективный современный метод, использующий измерения по фазе несущих в системе GPS, сходен с системой метеорной передачи времени, однако до настоящего времени находится в стадии технологического развития и в коммерческой эксплуатации не представлен.

Основные трудности использования метеорного канала связаны с неравноточностью и неравномерностью измерений. Если технология самих измерений достаточно отработана, то проблема управления шкалой времени в отсутствие измерений, актуальная для метеорного радиоканала, до настоящего момента не рассмотрена. Поэтому работа в области оптимизации использования неравномерных и неравноточных метеорных радиоизмерений для целей управления шкалами в реальном масштабе времени нуждается в развитии.

В использовании метеорного канала наметилась также новое направление—метеорный метод генерации ключей шифрования, который претендует на близкую к совершенной реализацию защиты информации при ее передаче на большие расстояния /3/. Метеорная генерация ключей шифрования опирается на достижения в области наносекундной синхронизации шкал времени с использованием метеорного канала, а также на его особенности, такие как сохранение взаимности условий распространения радиоволн с точностью до фазы несущей

при большом разбросе параметров распространения радиоволн для разных метеорных отражений. Высокая точность синхронизации шкал позволяет измерять случайные составляющие параметров метеорной радиолинии, изменяющиеся от отражения к отражению и использовать их, например, в качестве элементов ключа в шифре Вернама.

Таким образом изучение возможностей управления шкалой времени по неравномерным и неравноточным измерениям является актуальной современной научной проблемой и этой проблеме посвящена настоящая работа.

Целью диссертационной работы является разработка метода синхронизации шкал времени по метеорным радиоотражениям для управления шкалой времени с суб-наносекундной (0.3–1.0 нс) точностью в реальном масштабе времени для метрологических целей и метеорной защиты информации. Предполагается решение следующих задач:

1. Синтез модели системы управления шкалой времени с учетом физических свойств метеорного радиоканала и свойств используемых хранителей времени.

2. Обеспечение минимальной погрешности расхождения двух шкал времени в условиях автоматического управления вторичной шкалой по метеорному радиоканалу для преодоления кратковременной нестабильности квантовых стандартов частоты.

3. Построение метода и реализация алгоритма обеспечения однозначности фазовых измерений с использованием экспериментальных данных и оценка эффективности использования вариантов разнесения несущих частот в известном многочастотном фазовом методе передачи времени по метеорному радиоканалу.

4. Определение параметров метеорного радиоканала, необходимых для обеспечения наносекундной синхронизации шкал времени с учетом физических условий метеорного распространения радиоволн для целей передачи ключей шифрования в плане реализации идей метеорной криптографии.

Научная новизна работы заключается в следующем:

1. На основе идей оптимальной линейной фильтрации впервые разработана модель управления шкалой времени по неравномерным и неравноточным фазовым метеорным радиоизмерениям, включающая в себя модель хранителя времени, целевую функцию и модель измерений на основе радиофизических и статистических свойств метеорных отражений.

2. На основе разработанной модели проведена оценка потенциальной точности управления шкалой времени. Показано, что погрешность управления

не превышает значения 0.45 нс при использовании текущей оценки и 0.35 нс при использовании интервальной, задержанной во времени, оценки.

3. Впервые построен алгоритм преодоления неоднозначности фазовых измерений в системе передачи времени для различных вариантов максимального разноса несущих частот в многочастотном фазовом методе передачи времени по метеорному радиоканалу.

4. Даны количественные оценки производительности метеорного радиоканала с учетом возможных природных и аппаратурных ограничений при генерации ключей шифрования, используемых в целях защиты информации методами метеорной криптографии.

Практическая ценность работы определяется тем, что определены пути дальнейшего увеличения точности управления шкалой времени в диапазон долей наносекунд; дана количественная оценка потенциальной точности управления шкалой времени по метеорному радиоканалу, достижимая средствами современной аппаратуры. Результаты работы могут быть использованы для построения перспективных систем метеорной криптографии. Результаты могут быть также использованы для совершенствования метрологических систем хранения и передачи времени.

На защиту выносятся следующие положения:

1. Модель системы управления шкалой времени, использующая данные экспериментального аналога неравномерных и неравноточных фазовых измерений сдвига шкал времени по метеорному радиоканалу, учитывающая влияние кратковременной нестабильности хранителей времени и включающая в себя алгоритм разрешения неоднозначности фазовых измерений.

2. Количественная оценка потенциальной точности управления шкалой времени по метеорным радиоизмерениям, оцениваемая по стандартному отклонению ошибки оценки ухода вторичной шкалы времени по отношению к первичной, доступной как в реальном масштабе времени, так и с допустимой задержкой.

3. Метод и реализация алгоритма преодоления неоднозначности фазовых измерений в системе передачи времени для различных вариантов максимального разноса несущих частот в многочастотном фазовом методе передачи времени по метеорному радиоканалу.

4. Количественные оценки производительности метеорного радиоканала генерации ключей шифрования с учетом возможных природных и аппаратурных ограничений для различных вариантов принятия решений о смене режимов работы (передача времени/ключа).

Достоверность полученных результатов определяется применением известных оптимальных методов фильтрации; использованием в модели реальных измерений, выполненных на действующей аппаратуре; сопоставлением полученных результатов с результатами прямого измерения расхождения шкал времени на метеорной радиолинии.

Личный вклад автора Автором предложена методика управления шкалой времени, а также разрешения неоднозначности фазовых измерений ухода шкал на несущей частоте по результатам дискретной оптимальной линейной фильтрации. Автором разработана модель метеорного радиоканала генерации ключей шифрования, включающая в себя нестабильность КСЧ, неравномерные и неравноточные измерения по метеорным радиоотражениям, оригинальный способ увеличения длины ключевой последовательности с опорой на интервальную оценку сдвига шкал и возможность осуществления переспроса в метеорной системе связи. Для модельного описания неравномерных и неравноточных измерений автором был обработан имеющийся в КГУ экспериментальный материал по измерениям ухода шкал на метеорной радиолинии. Все предложенные автором методы реализованы в рамках единого специализированного пакета программного обеспечения с помощью которого проведен численный эксперимент по определению производительности метеорного радиоканала генерации ключей шифрования для различных вариантов построения системы метеорной синхронизации и генерации ключей.

Апробация работы и публикации. По теме диссертационной работы опубликовано 5 научных статей, в том числе 1 статья в журнале, включенном в перечень ВАК, 3 статьи по итогам международных конференций, 1 статья в региональной печати. По результатам диссертации автором опубликовано 7 работ.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав и заключения. В ней содержится 120 страниц печатного текста, приводится 27 рисунков и 1 таблица. Список литературы содержит 54 работы.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность диссертационной работы, ее цель, научная новизна и практическая значимость; формулируются положения, выносимые на защиту.

В первой главе рассматриваются основные особенности метеорного радиоканала, существенные для целей наносекундной передачи времени, показаны его достоинства и недостатки. Показана целесообразность использования метеорного канала для систем, в которых автономность и надежность имеют более важное значение, чем высокая пропускная способность, а также в которых существует необходимость использовать специфические условия существования канала. Кроме этого определены проблемы, обусловленные рядом физических

факторов, осложняющих как передачу времени, так и управление вторичной шкалой по метеорным радиоизмерениям. Приведены оценки экспериментально достижимой на сегодняшний день точности передачи времени по метеорному каналу, а также характеристики нестабильности современных квантовых стандартов частоты, поддерживающих шкалы времени. Показана возможность использования метеорного радиоканала для организации защищенного канала генерации ключей шифрования.

Управление шкалой времени по метеорному радиоканалу осложнено следующими его свойствами:

1. Случайностью появления регистрируемых метеорных отражений. Распределение случайных интервалов времени между появлением регистрируемых на заданной трассе метеорных отражений достаточно хорошо описывается экспоненциальным законом. Вследствие этого всегда существует вероятность появления чрезмерно длительного интервала времени, в течение которого измерения отсутствуют, что в частности усложняет относительную привязку неоднозначных фазовых измерений на несущей частоте. Эта проблема встает еще более остро при попытке отследить уход шкал вследствие кратковременной нестабильности квантовых стандартов частоты (КСЧ).

2. Неравноточностью измерений. Амплитуда сигнала и отношение сигнал/шум могут меняться в значительных пределах как в течение времени существования одного метеорного следа, так и от отражения к отражению. Кроме этого, зачастую в течение существования метеорного следа проводится множество последовательных измерений, результаты которых усредняются. Это также приводит к неравноточности получаемого одно-метеорного измерения т.к. случайные длительности отражений имеют распределение, близкое к экспоненциальному.

Возможность получения наносекундной точность передачи времени по метеорному радиоканалу была показана экспериментами, проходившими в КГУ в 1979-1981 гг. Эти эксперименты были поставлены с целью определить степень взаимности метеорного канала при использовании фазовых измерений. Взаимность канала есть одинаковость времени распространения сигнала по одному пути в прямом и обратном направлениях. Было показано, что ошибки невзаимности канала при передаче времени не превышают величины 0.3–0.5 нс и являются единственным фактором, ограничивающим потенциальную точность передачи времени по метеорному каналу. В последующей серии экспериментов 1987–1992 гг полученные результаты были подтверждены с использованием более совершенной аппаратуры метеорной синхронизации и более стабильного стандарта частоты.

Одним из применений скрытной связи, предоставляемой метеорным радиоканалом, в сочетании с наносекундной передачей времени, является генерация случайных чисел, которые можно использовать как ключи симметричного кода. Процедура генерации ключей предполагает измерение случайных параметров метеорных радиоотражений и использование их в качестве составляющих ключа шифрования. Если случайным параметром, используемым в качестве элемента ключа является время распространения сигнала на текущем метеорном отражении, то количество случайных бит, получаемых при его измерении, будет зависеть от ошибки текущей синхронизации шкал времени на корреспондирующих пунктах. Метеорный канал в этом случае используется в двух режимах, режиме передачи времени и режиме защищенного канала генерации ключей. Исключено при этом использование одного и того же метеорного отражения в двух режимах т.к. передача времени означает излучение в эфир информации о длине текущей метеорной линии.

Рациональное использование ограниченного, при конечной энергетике канала, количества регистрируемых метеорных отражений требует процедуры разделения во времени режимов синхронизации и генерации ключей. В то же время требуется производить оценку текущего ухода шкал как с целью обеспечения синхронности измерений, так и с целью получения и удержания однозначности фазовых измерений на несущей частоте. Случайность появления метеорных отражений в сочетании с кратковременной нестабильностью КСЧ при этом всегда оставляют возможными не только потерю наносекундной синхронизации, но и потерю привязки фазовых измерений на несущей, которая обеспечивает саму возможность осуществления наносекундной синхронизации.

Таким образом, являются актуальными вопросы учета влияния неравномерности и неравноточности фазовых измерений в метеорном радиоканале на обеспечение синхронности шкал времени в реальных условиях кратковременной нестабильности КСЧ и ограниченного количества метеорных отражений, используемых для передачи времени.

Вторая глава посвящена описанию интерпретации результатов эксперимента по метеорной привязке шкал времени из серии проведенных в КГУ с 1988 по 1993 гг. Эксперимент проходил на трассе Менделеево(Моск.обл)–Казань с использованием фазовой аппаратуры метеорной синхронизации и связи "Кама–5", разработанной в КГУ. Аппаратура имеет несколько особенностей, отражающих использованный метод метеорной синхронизации. 1) эффективное исключение из результатов измерения времени распространения радиоволн при двухсторонней передаче сигналов 2) многочастотный фазовый метод передачи времени 3) низкий порог регистрации метеорных отражений

Основные параметры аппаратуры и эксперимента были следующими: Длина трассы: 720 км; Средняя мощность передатчика: 500 Вт в режиме передачи, 200 Вт в режиме ожидания; Используемая полоса частот: 4 канала шириной

25 КГц, с максимальным разносом частот 500 КГц; Точность измерения на одном метеорном следе: 14–18 нс по однозначному измерению фазы максимальной разностной частоты, 0.3 нс по неоднозначному измерению фазы несущей; кратковременная нестабильность цезиевого стандарта частоты (интервал 1 сек): $\sigma_{\Delta f/f} = 5.6 \cdot 10^{-11}$.

Отличительной особенностью использованных экспериментальных данных являлось то, что по ним можно было точно оценить шумовую погрешность измерений для большинства зарегистрированных метеорных отражений. Кроме того, данные эксперимента содержат информацию о фазовых измерениях на нескольких несущих, что можно использовать при пересчете величин ошибок измерений для других вариантов разнесения частот. Распределение стандартных отклонений шумовых ошибок измерений на одном метеорном отражении показано на рис. 1.

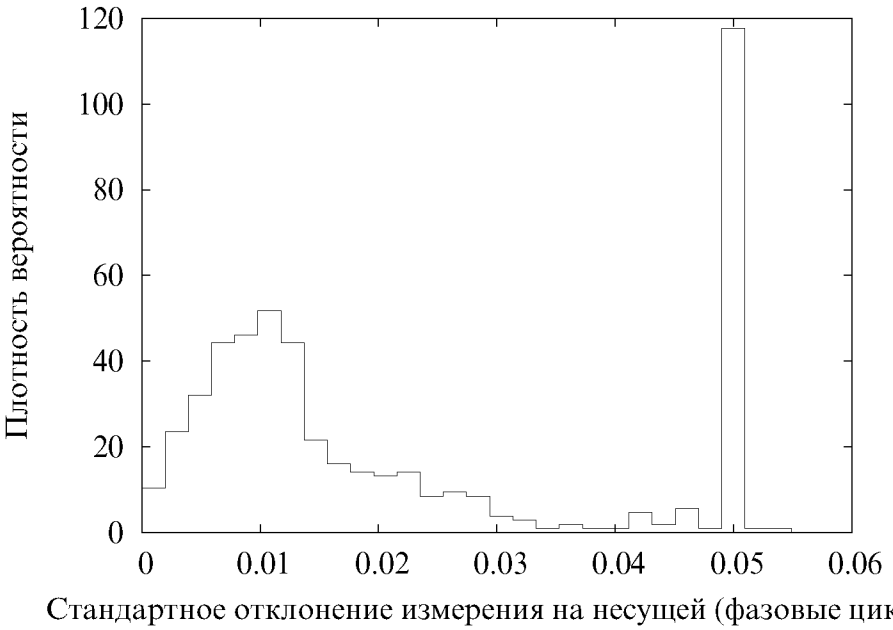

Рис. 1. Распределение стандартных отклонений измерений ухода шкал по фазе несущей частоты

Кратковременная нестабильность цезиевых стандартов хорошо описывается белым частотным шумом на всем интересующем нас интервале—от единиц секунд до нескольких часов. Таким образом двухвыборочная дисперсия (Аллена) может быть использована как дисперсия относительного отклонения частоты от номинала как при фильтрации экспериментальных данных, так и в модели, использующей экспериментально полученное распределение ошибок измерений.

В третьей главе описывается модель управления шкалой времени по метеорным радиоизмерниям. Данная модель необходима как для описания исследуемых процессов управления шкалой в терминах оптимальной линейной фильтрации, так и для компьютерного моделирования, необходимого при иссле-

довании алгоритмов принятия решений на ее основе. Построение модели требует правильного описания и учета случайных процессов, оказывающих влияние на результирующую точность управления шкалой: неравномерность и неравноточность измерений в условиях нестабильности исследуемого процесса. Для учета этих процессов хорошо подходит использование оптимальной линейной фильтрации для случая систем с дискретными измерениями. Этот подход удобен по ряду причин: 1) исследуемый случайный процесс (уход шкал) оценивается по дискретным измерениям в моменты появления регистрируемых метеорных отражений, 2) ошибки измерений полагаются гауссовскими, причем необходимые значения параметров распределения для каждого измерения, как на несущей так и на максимальной разностной частотах, легко находятся из экспериментальных данных по измерениям на несущей, 3) допустимым является предположение о независимости измерений, что обусловлено пространственным разделением метеорных следов и случайностью их положения, 4) нестабильность используемого цезиевого КСЧ хорошо описывается частотным белым гауссовским шумом, значение которого берется из описания стандарта частоты и легко вносится в уравнение фильтра. Присутствует также проблема, не решаемая оптимальной линейной фильтрацией: неоднозначность фазовых измерений на несущей. Необходимым является связать процедуру оптимальной линейной фильтрации доступных однозначных измерений с проблемой перехода к фазе несущей и обеспечения таким образом максимально возможной точности измерений.

Фазовое измерение сдвига шкал на текущем метеорном следе описывается следующим образом. Измерение содержит два типа ошибок: шумовую ошибку и ошибку невзаимности канала на текущем пути распространения сигналов. Шумовая ошибка различна для всех используемых несущих. Неустранимая, на момент проведения эксперимента, остаточная ошибка невзаимности связана главным образом с ветровым смещением метеорного следа. Такая ошибка одинаково проявляется на всех несущих частотах и практически не изменяется в течение существования метеорного следа, однако может различаться для разных отражений.

Измерение фазы удвоенного (особенность двухсторонней передачи сигналов) сдвига шкал запишется следующим образом:

$$\phi_k^j = \|2f_j(\tau_k + \epsilon_k) + \theta_j(\sigma_k)\|,$$

где τ_k—сдвиг шкал в момент появления k-го метеорного отражения, f_j—j-я несущая частота, $\theta_j(\sigma_k)$—ошибка текущего измерения по фазе несущей, ϵ_k—ошибка невзаимности канала для текущего измерения. $\|\cdot\|$ означает отбрасывание целой части: $\|a\| = a - \lfloor a \rfloor$.

Уход шкал вследствие нестабильности стандарта частоты будет записан как:

$$\tau(t) = \tau_0 + \frac{\Delta f}{f_0} t + \int_0^t \rho dt,$$

где $\rho(t)$ – случайный процесс, описывающий частотный шум стандарта частоты, τ_0 – сдвиг шкал в начальный момент времени, f_0 – номинальная частота стандарта, Δf_0 – систематическая составляющая сдвига частоты стандарта от номинальной. Для использования в уравнениях дискретной фильтрации удобнее представить относительный уход шкал в виде

$$\tau_k = \left(\gamma_{k-1} + \frac{\Delta f}{f_0}\right)(t_k - t_{k-1}) + \tau_{k-1},$$

где где τ_k – сдвиг шкал на момент t_k текущего измерения, γ_{k-1} – случайная величина, представляющая шумовой сдвиг шкал накопленный с момента t_{k-1} до момента t_k. Дисперсия случайной величины γ_k может быть представлена либо с использованием величины дисперсии Аллена $\sigma^2_{\frac{\Delta f}{f}}(dt_k)$ (паспортная характеристика), либо представлена в виде $N_0/2dt_k$, где спектральная плотность мощности частотного шума $N_0/2$ вычисляется по величине $\sigma^2_{\frac{\Delta f}{f}}(1)$.

Оптимальная линейная фильтрация предполагает представление рассматриваемого процесса в виде системы матричных уравнений:

$$\begin{aligned} x(k+1) &= F(k+1,k)x(k) + G(k+1,k)w(k) \\ z(k+1) &= H(k+1)x(k+1) + v(k+1), \end{aligned}$$

где x—n-вектор состояния; w—p-вектор возмущения; z—m-вектор измерения; v—m-вектор ошибки измерения; $k = 0, 1\ldots$–дискретное время; F—переходная матрица состояния размера $n \times n$; G—переходная матрица возмущения размера $n \times p$; H—матрица измерения размера $m \times n$.

Вектором состояния в нашей системе будет

$$\begin{pmatrix} \tau \\ \frac{\Delta f}{f_0} \end{pmatrix}_{k+1} = \begin{pmatrix} 1 & dt_k \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \tau \\ \frac{\Delta f}{f_0} \end{pmatrix}_k + \begin{pmatrix} 0 & dt_k \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ \gamma \end{pmatrix}_k,$$

где τ—величина текущего сдвига шкал, $\frac{\Delta f}{f}$—постоянное отклонение частоты стандарта от номинала.

Вектор измерения (в нашем случае скаляр) запишется как

$$Z_{k+1} = \begin{pmatrix} 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} \tau \\ \frac{\Delta f}{f} \end{pmatrix}_{k+1} + V_{k+1},$$

где V_{k+1}—ошибка текущего измерения удвоенного сдвига шкал.

При использовании модели в численном эксперименте последовательно генерируются следующие величины: 1) Сдвиг шкал $\tau_{k+1} = \tau_k + \frac{\Delta f}{f_0} dt_k + \gamma_k$, где γ_k - случайная величина с гауссовским распределением, нулевым средним и дисперсией $N_0/(2dt_k)$ 2) Ошибка невзаимности текущего измерения ϵ_k, как гауссовски распределенная случайная величина со стандартным отклонением 0.3 нс. Данную ошибку считаем одинаковой для каждой несущей. 3) Стандартное отклонение текущего измерения удвоенного сдвига шкал по фазе несущей σ_k,

генерируется по распределению, полученному в эксперименте (рис. 1). 4) Фазовые измерения удвоенного сдвига шкал ϕ_k^0 и ϕ_k^1, соответствующие максимально разнесенным частотам f_0 и f_1. 5) Измерения сдвига шкал по фазе максимальной разностной частоты вычисляются как $M_\tau^d = \frac{\phi_1 - \phi_0}{f_1 - f_0}$, причем к величине M_τ^d добавляется необходимое количество периодов однозначности, что имитирует процедуру последовательного разрешения неоднозначности фаз разностных частот. Предполагается, что наиболее уязвимым для ошибок является переход от фазы максимальной разностной частоты к фазе несущей, что обусловлено возможностью выбора соотношения несущих. Достижение однозначной фазы максимальной разностной частоты считаем осуществимым и безошибочным.

Управление шкалой времени вторичного стандарта в рамках работы осуществляется путем введения поправок непосредственно в шкалу времени в виде ее смещения. Поправка вычисляется на основании результатов оптимальной линейной фильтрации измерений и вводится мгновенно, по принятии решения о ее необходимости. Таким образом, величина ошибки управления определяется величиной ошибки оптимальной оценки на момент принятия этого решения.

Четвертая глава посвящена синтезу методов управления шкалами времени применительно к различным задачам и их технической реализации. Наиболее важной задачей является оценить производительность метеорного канала генерации ключей шифрования при наличии и отсутствии ограничений, связанных со стохастическими свойствами метеорных отражений.

В первую очередь рассмотрен вопрос о потенциальной точности управления шкалой времени на аппаратуре метеорной синхронизации, использующей технические решения на основе фазовой аппаратуры "Кама". Здесь требуется ответить на вопрос: каким может быть расхождение шкал в *случайный* момент времени после начала работы аппаратуры синхронизации, независимо от наличия или отсутствия в этот момент метеорного следа. При этом предполагается что время передается при наличии метеорного следа с точностью, обеспечиваемой измерением фазы несущей частоты, а отслеживание и разрешение неоднозначности измерений на несущей происходит безошибочно. Главной исследуемой характеристикой является ошибка фильтрации, как текущей, так и интервальной. Ошибкой управления будет ошибка прогноза ухода шкал, а остаточная ошибка, в тех случаях где можно отложить принятие решений об управлении—ошибка задержанной во времени интервальной оценки. Точность управления в случайный момент времени удобно представить в виде распределения ошибок оптимальной линейной оценки.

Далее рассмотрены возможные варианты принятия решений о разрешении неоднозначности измерений по фазе несущей с опорой на независимую оценку фильтрации разностных измерений и предложен алгоритм разрешения неоднозначности в условиях использования метеорного канала в качестве канала генерации ключей шифрования.

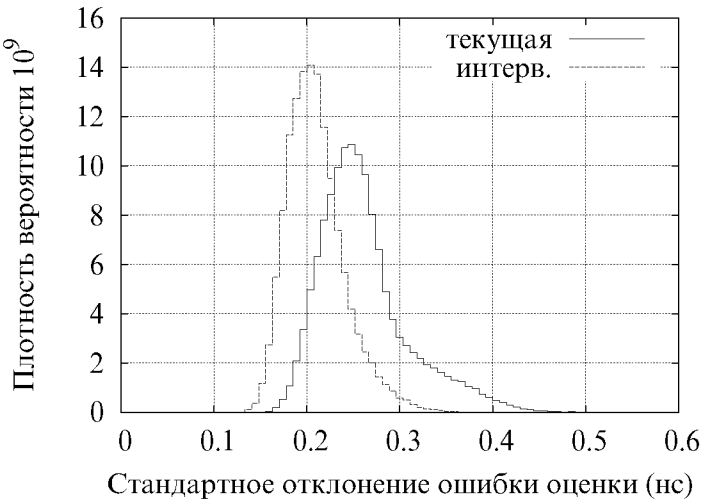

Рис. 2. Распределение стандартных отклонений ошибок оценки текущего сдвига шкал времени (120 регистрируемых отражений в час)

Для оценки производительности метеорного канала генерации ключей шифрования сначала рассмотрим наиболее простую задачу получения максимально доступного количества бит ключа путем измерения полного времени распространения сигнала при отсутствии необходимости разрешать неоднозначность фазовых измерений на несущей частоте. Производительность канала генерации ключей шифрования определяется здесь только свойствами метеорных отражений, неопределенностью времени распространения волн по текущему пути и точностью синхронизации. Решение о переходе от режима передачи времени в режим измерения времени распространения сигналов и наоборот принимается по пороговому значению ошибки текущей оценки сдвига шкал. Если ошибка оценки текущего сдвига шкал возрастает в отсутствие синхронизационных измерений и выходит за пределы порогового уровня аппаратура переходит в режим синхронизации. В остальных случаях передается сигнал, позволяющий определить случайную составляющую текущей длины трассы, причем количество получаемых бит ключа зависит от текущей ошибки оценки сдвига шкал. Использование порогового уровня величины ошибки текущей оценки позволяет сделать распределение синхронизационных измерений более равномерным, что положительно сказывается на равномерности поведения ошибки оценки т.к. интервалы между измерениям становятся приблизительно одинаковой длительности. Количество бит, передаваемых на одном следе в режиме передачи данных есть логарифмическая функция текущей ошибки оценки сдвига шкал. Возможность использования интервальной (задержанной во времени) оценки сдвига шкал при этом определяется наличием в метеорной аппаратуре системы переспроса, позволяющей ведомому пункту по прошествии необходимого времени накопления уведомить ведущий о новом, более точном значении ошибки сдвига шкал на момент генерации ключа.

Предел измерения точности сдвига шкал в метеорном радиоканале определяется остаточной фазовой невзаимностью канала (0.3 нс). Мы можем использовать следующую функцию количества передаваемых бит на одном следе N от стандартного отклонения ошибки σ оценки сдвига шкал:

$$N(\sigma) = \lfloor \log_2 \frac{\tilde{T}}{a\sigma} \rfloor,$$

где, $\tilde{T}$—величина разброса случайной составляющей времени распространения сигнала (в данном случае 500 мкс), а коэффициент a соответствует требуемой вероятности ошибки передачи ключа. Например, величина $a = 6$ соответствует вероятности ошибки получения ошибочного младшего бита ключа 0.003, что для максимально возможной точности сверки шкал (ошибка 0.3 нс) дает 18 бит ключа.

Зависимость скорости передачи ключа от порогового уровня перехода в режим передачи времени показана на рис. 3. Видно, что скорость передачи

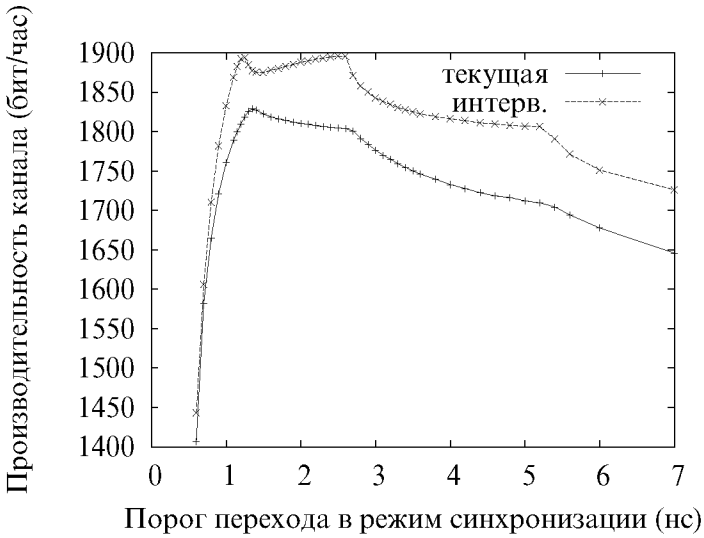

Рис. 3. Средняя скорость передачи ключа в зависимости от порога перехода в режим передачи времени.

ключа достигает 0.5 бит/сек по текущей оценке и незначительно увеличивается при использовании интервальной оценки. Порог, при котором скорость передачи близка к оптимальной, соответствует относительно нечастым синхронизационным измерениям. На каждое отражение, использованное для синхронизации, приходится в среднем 15-20 передач ключа. На данном этапе для успешного обмена ключами нет принципиальной необходимости получать малые (0.5-1.0 нс) ошибки синхронизации. Это связано с предположением о возможности без ограничений измерять случайную составляющую времени распространения сигналов по метеорному радиоканалу.

Измерение полного времени распространения сигналов на текущем метеорном следе является нежелательной процедурой по причине того, что условия воз-

можности его осуществления (последовательное разрешение неоднозначности фаз разностных частот) совпадают с условиями успешного перехвата информации криптоаналитиком в зоне, находящейся вблизи пунктов приема. Максимальное уменьшение зоны возможного прослушивания защищенного канала требует использования несущих частот, выбранных таким образом, чтобы обеспечивать независимость фазовых измерений времени распространения. Количество бит ключа, получаемого при этом по неоднозначному измерению на одной частоте, определяется величиной ее периода, точностью ее измерения и величиной ошибки текущей синхронизации. В дальнейшем предполагаем, что ошибка измерения фазы несущей несущественна в режиме передачи ключа, так как она по крайней мере не должна быть меньше ошибки, получаемой при измерении времени. Учитывая что передача ключей происходит как раз в моменты отсутствия синхронизационных измерений, понятно, что основной вклад в ошибку вносит расхождение шкал. В выражении для количества передаваемых бит на одном следе N от стандартного отклонения ошибки σ оценки сдвига шкал величина $\tilde{T}$ будет равняться периоду несущей частоты. Использование K рабочих частот позволяет увеличить количество переданных бит ключа в K раз. Отказ же от процедуры последовательного разрешения неоднозначности фаз разностных частот позволяет уменьшить зону возможного пассивного прослушивания канала до 100–150 метров /3/. В то же время каждая дополнительная несущая приближает общее количество бит, переданных на одном следе к величине 18–19 бит, обеспечиваемой неоднозначностью длины текущего пути распространения волн, измеренного с суб-наносекундной точностью. На рис. 4 показаны зависимости производительности канала передачи ключа при использовании во встречном режиме одной несущей от величины порога принятия решения о переходе в режим синхронизации. Графики приведены для различных величин количества регистрируемых отражений в час. Для сравнения также показаны значения производительности канала, получаемые при использовании текущей оценки.

Наиболее сложным случаем является генерация ключей при ограниченном максимальном частотном разносе, что не позволяет разрешать неоднозначность измерений на несущей непосредственно в течение существования одного метеорного отражения. В этом случае задачу можно представить как распределение метеорных отражений для трех целей: 1) передача времени для уточнения шкалы времени, 2) передача времени с целью поддержания однозначности (и высокой точности) измерений времени, 3) передача ключей. Алгоритм, предложенный для решения этой задачи предполагает использование двух фильтров для фильтрации соответственно измерений по максимальной разностной частоте, и измерений на несущей. Окончательное решение о возможности перехода к фазе несущей и точности результирующих измерений времени распространения (бит ключа) определяется по величине ошибки интервальной оценки фильтра разностных измерений. Производительность канала для случая максимального

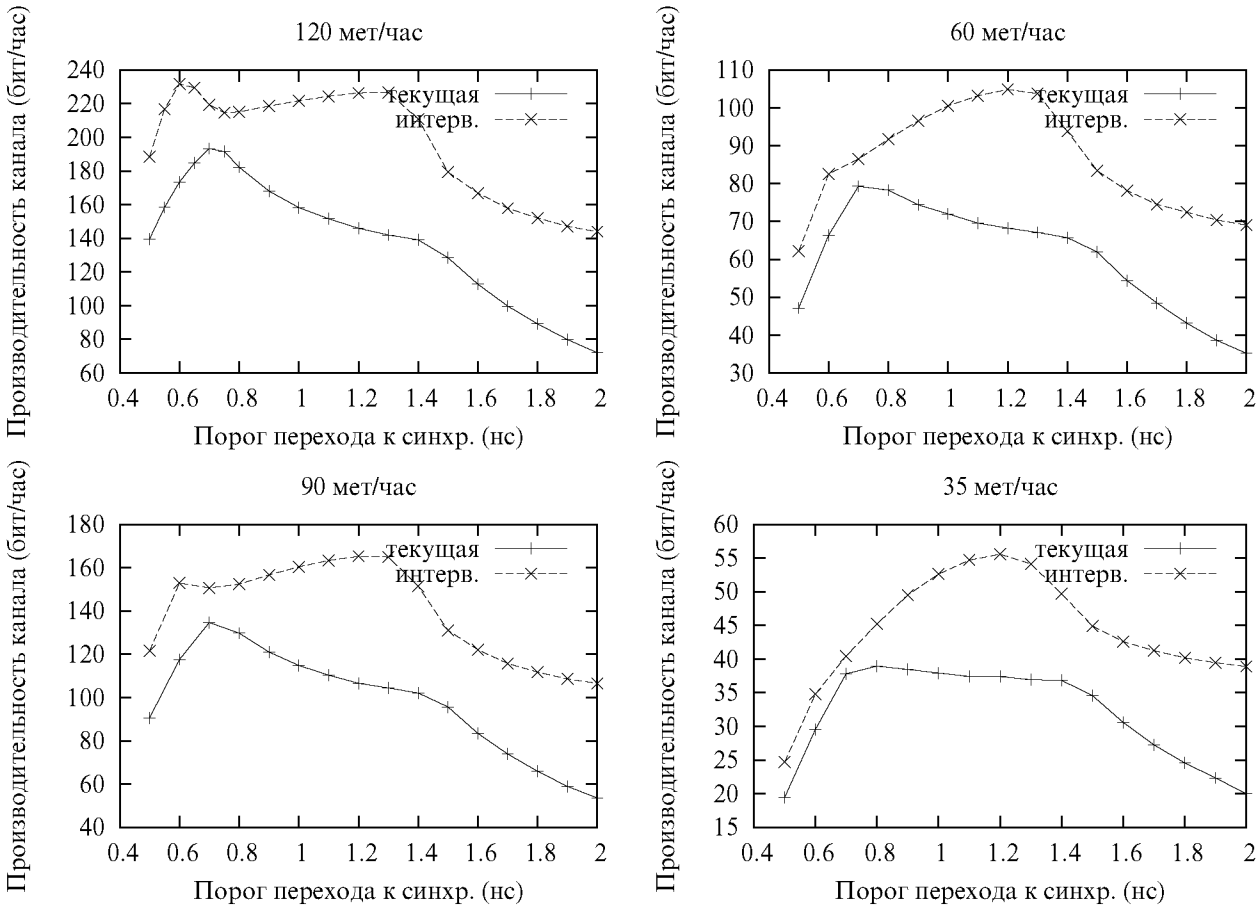

Рис. 4. Производительность канала передачи ключей, использующего одну несущую, для различных значений среднего количества отражений в час

разнесения частот 2.5 МГц приведена на рис. 5. В результирующую производительность включена также величина ошибочных бит ключа, полученных из-за неправильного определения номера периода однозначности несущей. Отдельно на графиках приведен также вклад ошибочных измерений.

В заключении приведены основные результаты диссертации:

1. Разработан метод управления шкалой времени с наносекундной точностью по неравноточным и неравномерно поступающим фазовым радиометеорным измерениям, обеспечивающий возможность отслеживания ухода шкал вследствие кратковременной нестабильности квантовых стандартов частоты. Метод использует результаты оптимальной линейной фильтрации дискретных во времени фазовых измерений, которая учитывает как шумы измерений, так и нестабильность отслеживаемого ухода шкал, и позволяет использовать их в частности для разрешения неоднозначности фазовых измерений на несущей частоте. В качестве экспериментального аналога в численных экспериментах использованы имеющиеся в КГУ дан-

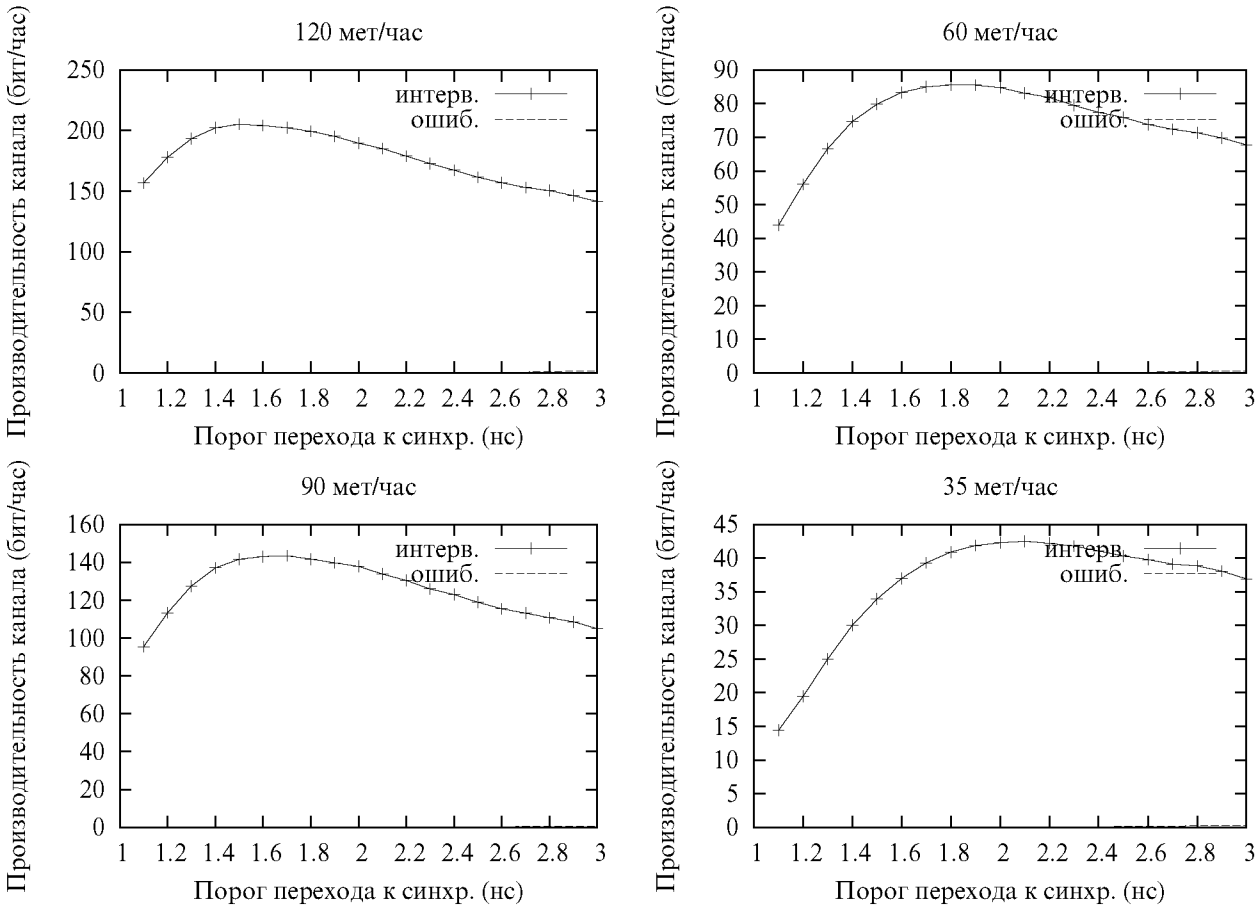

Рис. 5. Производительность канала передачи ключей, использующего одну несущую и ограниченный (2.5 МГц) максимальный разнос частот, для различных значений среднего количества отражений в час

ные измерений расхождения шкал времени на многочастотной фазовой аппаратуре "Кама-5" на трассе Менделеево(Моск. обл)–Казань, 1992 г.

2. По результатам фильтрации моделируемых фазовых измерений на несущей частоте оценена потенциальная точность управления шкалой времени в случае использования всех доступных метеорных отражений для синхронизации при энергетике канала, обеспечивающей среднее количество регистрируемых метеорных отражений 35–120 мет/час. Распределение ошибок управления шкалой времени показывает, что в процессе управления шкалы сведены с погрешностью 0.5–1.3 нс в зависимости от количества регистрируемых метеорных отражений уже по текущей оценке. Ошибка интервальной оценки при этом не превышает 0.35–0.8 нс.

3. Предложены возможные алгоритмы принятия решений о переходе к несущей с опорой как на независимые оценки фильтрации разностных измерений, так и с использованием ряда оценок, зависящих от выполненных

ранее разрешений неоднозначности измерений на несущей. Один из предложенных вариантов был использован при управлении шкалой времени в численном эксперименте по определению производительности метеорного канала генерации ключей шифрования при ограниченном максимальном разносе несущих частот.

4. Показана принципиальная возможность совмещения процедур автоматического поддержания шкал времени и передачи данных (генерации ключей шифрования) для целей метеорной криптографии в одном метеорном радиоканале. Предложена процедура принятия решений о переходе метеорной системы генерации ключей шифрования в режим передачи времени в условиях ограниченного максимального частотного разноса, которая предполагает опору на текущую оценку фильтрации разностных измерений и возможность как увеличения информационной значимости, так и отбрасывания переданных ранее ключей шифрования посредством системы переспроса по результатам запаздывающей интервальной оценки. Оценена производительность метеорной системы генерации ключей шифрования для различных вариантов максимального частотного разноса и энергетических параметров радиолинии определяющих численность регистрируемых метеорных отражений.

Основное содержание диссертационной работы изложено в следующих публикациях:

1. Корнеев В.А. Использование фильтра Калмана для управления шкалой времени по неравномерным и неравноточным измерениям по метеорному радиоканалу. [Текст] / В.А. Корнеев, В.В. Сидоров, Л.А. Эпиктетов // Прием и обработка информации в сложных информационных системах. — Казань, 2002, Выпуск 20, Изд-во: КГУ. — с. 88.

2. Корнеев В.А. Исследование времени однозначного перехода к фазе несущей при автоматическом управлении шкалой времени по измерениям в метеорном радиоканале. [Текст] / В.А. Корнеев, В.В. Сидоров, Л.А. Эпиктетов // Известия вузов. Радиофизика. — 2003 — Том XLVI № 12. — с. 1044-1050.

3. Sidorov V.V. Meteor Time Transfer and Meteor Cryptography [Text] / V.V. Sidorov, A.V. Karpov, V.A. Korneev, A.F. Nasyrov — по итогам конференции 21^{st} European Frequency and Time Forum (TimeNav'07), Geneva, 29 May–1 June 2007. *http://ieeexplore.ieee.org/iel5/4318993/4318994/04319088.pdf?tp=&arnumber=4319088&isnumber=4318994*

4. Korneyev V.A. Time & Frequency coordination using unsteady, variable-precision measurements in meteor burst channel [Text] / V.A. Korneyev,

L.A. Epictetov, V.V. Sidorov // Proc. of 17^{th} European Frequency and Time Forum — Tampa, USA, May 4–7 June 2003 — p. 186.

5. Korneyev V.A. Time & Frequency coordination using unsteady, variable-precision measurements in meteor burst channel [Text] / V.A. Korneyev, L.A. Epictetov, V.V. Sidorov // по итогам конференции 17^{th} European Frequency and Time Forum — Tampa, USA, May 4–7 June 2003. *http://www.ieee-uffc.org/archive/fc/proceed/2003/proceed/s0310285.pdf*

6. Korneev V.A. Optimization of concurrent data and high-precision time transfer modes in meteor burst synchronization equipment [Text] / V.A. Korneev, V.V. Sidorov по итогам конференции 21^{st} European Frequency and Time Forum (TimeNav'07), Geneva, 29 May–1 June 2007. *http://ieeexplore.ieee.org/iel5/4318993/4318994/04319214.pdf?tp=&arnumber=4319214&isnumber=4318994*

7. Корнеев В.А. Моделирование условий управления шкалами времени квантовых стандартов частоты по метеорному радиоканалу. [Текст] / В.А. Корнеев, В.В. Сидоров, Л.А. Эпиктетов // Труды XX всероссийской конференции по распространению радиоволн. Ниж. Новгород 2–4 июля 2002 с. 495–496.